

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An encryption device for encrypting information on a confidential target, comprising:

an imaging unit configured to perform imaging on a target and to output a first and second signal, said first signal including image data of an inside portion of the target, and said second signal including variation patterns specific to the imaging unit;

an identification unit configured to perform analog/digital conversion on the first signal having the image data to create identification information;

a creation means for creating a unique parameter of an element group based on a signal output from the element group internally having a plurality of elements as a unit configured to perform analog/digital conversion on the second signal having the variation patterns to create encryption key information; and

an encryption means for encrypting the unit configured to encrypt the identification information by using the unique parameter encryption key information created by the creation means.

Claim 2 (Currently Amended): The encryption device according to claim 1, wherein the creation means comprises unit includes a storage means for storing unit configured to store a plurality of different predetermined evaluation patterns having different hamming distances, and creates a combination of correlation values between the signal and the evaluation patterns being stored in the storage means, as the unique parameter said creation unit is further configured to create the encryption key information by using at least one calculated hamming distance of the image data and the different evaluation patterns.

Claim 3 (Currently Amended): The encryption device according to claim 2, further comprising:

a communication means for communicating unit configured to communicate with a prescribed communication party, wherein and

the creation means selects unit is further configured to select evaluation patterns requested by the communication party, from the evaluation patterns ~~being~~ stored in the storage ~~means unit, and creates a combination of correlation values between the signal and the evaluation patterns selected, as the unique parameter.~~

Claims 4 and 5 (Canceled).

Claim 6 (Currently Amended): An encryption method for encrypting information on a confidential target, comprising:

performing imaging on an inside portion of a target via an imaging unit;  
outputting a first signal that includes image data of the inside portion of the target;  
outputting a second signal that includes variation patterns specific to the imaging unit;  
performing analog/digital conversion on the first signal having the image data to  
create identification information;

performing analog/digital conversion on the second signal having the variation  
patterns to create encryption key information a first step of creating a unique parameter of an  
element group based on a signal output from the element group internally having a plurality  
of elements as a unit; and

a second step of encrypting via a processor the identification information by using the  
unique parameter created encryption key information.

Claim 7 (Currently Amended): The encryption method according to claim 6, ~~wherein the first step creates a combination of correlation values between the signal and further comprising:~~

storing a plurality of different predetermined evaluation patterns having different hamming distances, as the unique parameter; and

creating the encryption key information including calculating at least one hamming distance of the image data and the different evaluation patterns.

Claim 8 (Currently Amended): The encryption method according to claim 7, ~~wherein, the first step selects further comprising:~~

selecting evaluation patterns meeting to a request made from requested by a prescribed communication party[[],] from the evaluation patterns and creates a combination of correlation values between the signal and the evaluation patterns selected as the unique parameter being stored.

Claims 9 and 10 (Canceled).

Claim 11 (New): An encryption device for encrypting information on a confidential target, comprising:

imaging means for performing imaging on a target and outputting a first and second signal, said first signal including image data of an inside portion of the target, and said second signal including variation patterns specific to the imaging means;

identification means for performing analog/digital conversion on the first signal having the image data to create identification information;

creation means for performing analog/digital conversion on the second signal having the variation patterns to create encryption key information; and  
encryption means for encrypting the identification information by using the encryption key information.

**Claim 12 (New):** The encryption device according to claim 1, wherein said imaging unit is further configured to project near-infrared light into the target.

**Claim 13 (New):** The encryption device according to claim 13, wherein the first signal includes blood vessel pattern information representing a formation pattern of blood vessel tissues inside the target.

**Claim 14 (New):** The encryption device according to claim 1, wherein said second signal includes data based on a signal output from a piezoelectric element of a touch pad.

**Claim 15 (New):** The encryption device according to claim 1, wherein said second signal includes data of a group of active elements.

**Claim 16 (New):** The encryption device according to claim 1, wherein said second signal includes data of a group of passive elements.